**北京邮电大学软件学院**

**2017-2018 学年第 1学期实验报告**

**课程名称： 计算机网络\_\_\_\_\_\_\_\_**

**实验名称： 数据链路层实验\_\_\_\_\_\_\_**

**实验完成人：**

**姓名：**\_\_\_\_田宇\_\_\_\_**学号：**\_\_\_\_\_2016212011\_\_\_

**成绩：**\_\_\_\_\_\_\_\_

**指导教师：**\_\_\_\_\_\_\_ \_\_**\_\_王文东\_**\_\_\_\_\_\_\_\_\_\_\_\_\_\_

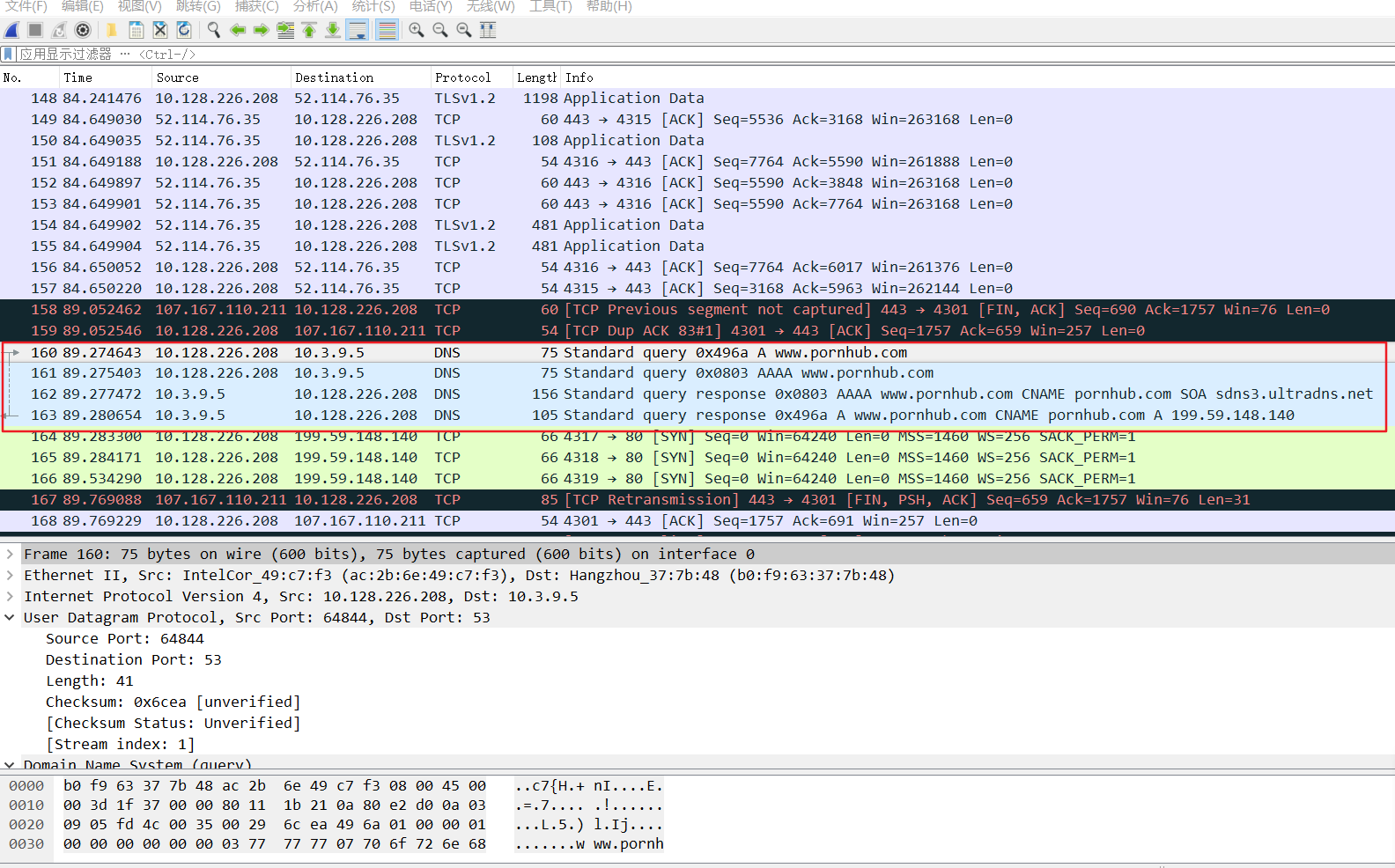
**日 期： 2018 年 11 月 1 日**

1. **实验目的**

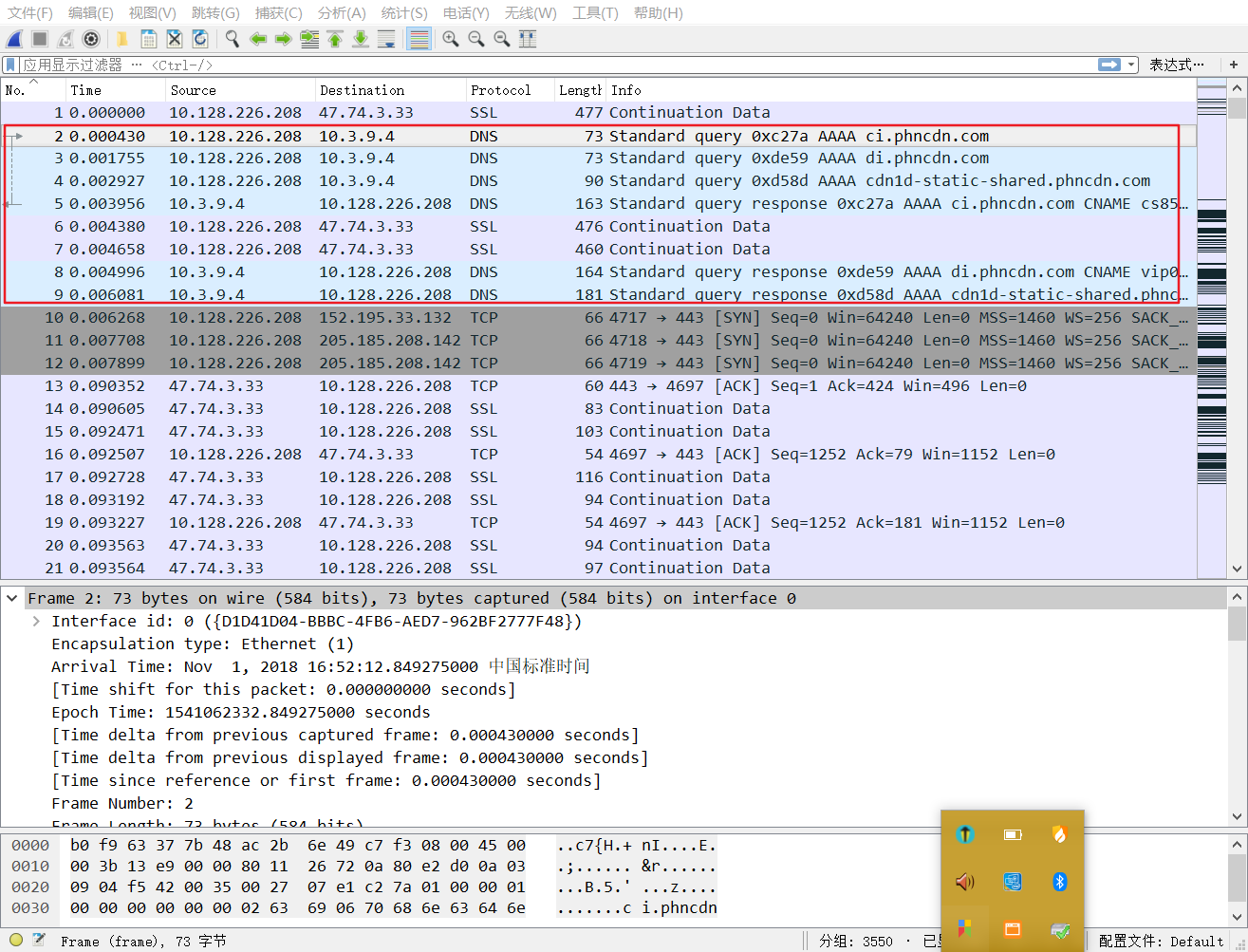
通过本实验使学生理解数据链路层协议数据单元（PDU）的定义和数据链路层功能。

1. **实验内容**
   1. 使用网络协议分析软件Wireshark抓取本计算机访问某网站（例如北京邮电大学网站，其网址为http://www.bupt.edu.cn）时发送和接收到的数据包；
   2. 对所抓取的数据包进行分析，分析数据链路层的帧结构及各字段的含义。
   3. 选做内容：分析实验中抓取的DNS（Domain Name System）消息、HTTP消息、TCP报文和IP分组，分析TCP报文字段组成及含义，分析IP分组的字段组成及含义。
2. **实验环境**
   1. Windows操作系统
   2. Wireshark：Wireshark是一个开源的抓包工具。
3. **实验步骤**
   1. 启动计算机上安装的Wireshark程序。
   2. 点击Wireshark程序主窗口的“Capture ”菜单项，选中该下拉菜单中的“Options”菜单项，通过出现的“Capture Options”窗口中的“Interface”选择框设置需要抓取哪个网卡发送/接收的数据包。
   3. 可通过“Capture Options”窗口中的“Capture Filter”选择框设置需要抓取的数据包的类型，比如选择“IP only”。
   4. 点击“Capture Options”窗口中的“start”按钮，启动抓包工作。此时可看见Wireshark程序出现了一个新的窗口：“Capturing”窗口。
   5. 启动本计算机中的浏览器程序（IE浏览器或Firefox浏览器），在浏览器的地址栏中输入所要访问的网站的网址（例如北京邮电大学的网址<http://www.bupt.edu.cn>）后按回车键，可看到浏览器中出现该网站的主页。
   6. 在Wireshark程序的“Capturing”窗口中观察Wireshark程序抓取的数据包；该窗口中的每一条记录为本机发送或接收到的一个数据包；
   7. 鼠标双击“Capturing”窗口中的一条记录，出现展示该数据包详细信息的窗口。在该窗口下面部分的子窗口中有该数据包（数据链路层帧）的二进制数据表示；在该窗口上面部分的子窗口中有Wireshark程序对该帧的分析，详细列出了该帧的字段组成以及各字段的取值。观察该帧的“Destination”字段、“Source”字段、“Type”字段的取值，以及该帧携带的数据。在实验报告中分析数据链路层帧的字段组成和作用。
   8. 观察“Capturing”窗口显示的所抓取的数据包，分析哪些数据包是发送出去的数据包，哪些数据包是接收到的数据包。
   9. 分析所抓取的数据包中的DNS（Domain Name System）协议消息过程、HTTP协议消息过程、TCP连接建立过程，分析TCP报文字段组成及含义，分析IP分组的字段组成及含义。
4. **实验过程及结果**

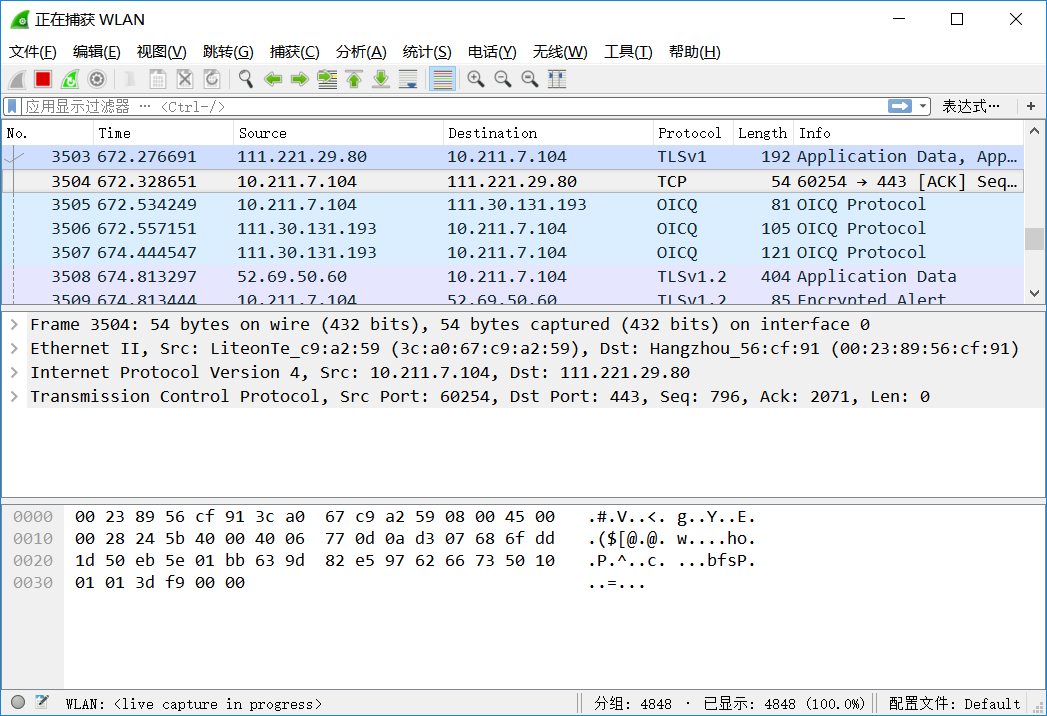
抓取计算机浏览国外成人视频网站PornHub网址<http://www.>pornhub.com时发送接收的数据包：（未开启VPN所以并没有加载出页面）



抓取计算机浏览成人视频网站PornHub网址<http://www.>pornhub.com时发送接收的数据包：（开启VPN加载出了页面）

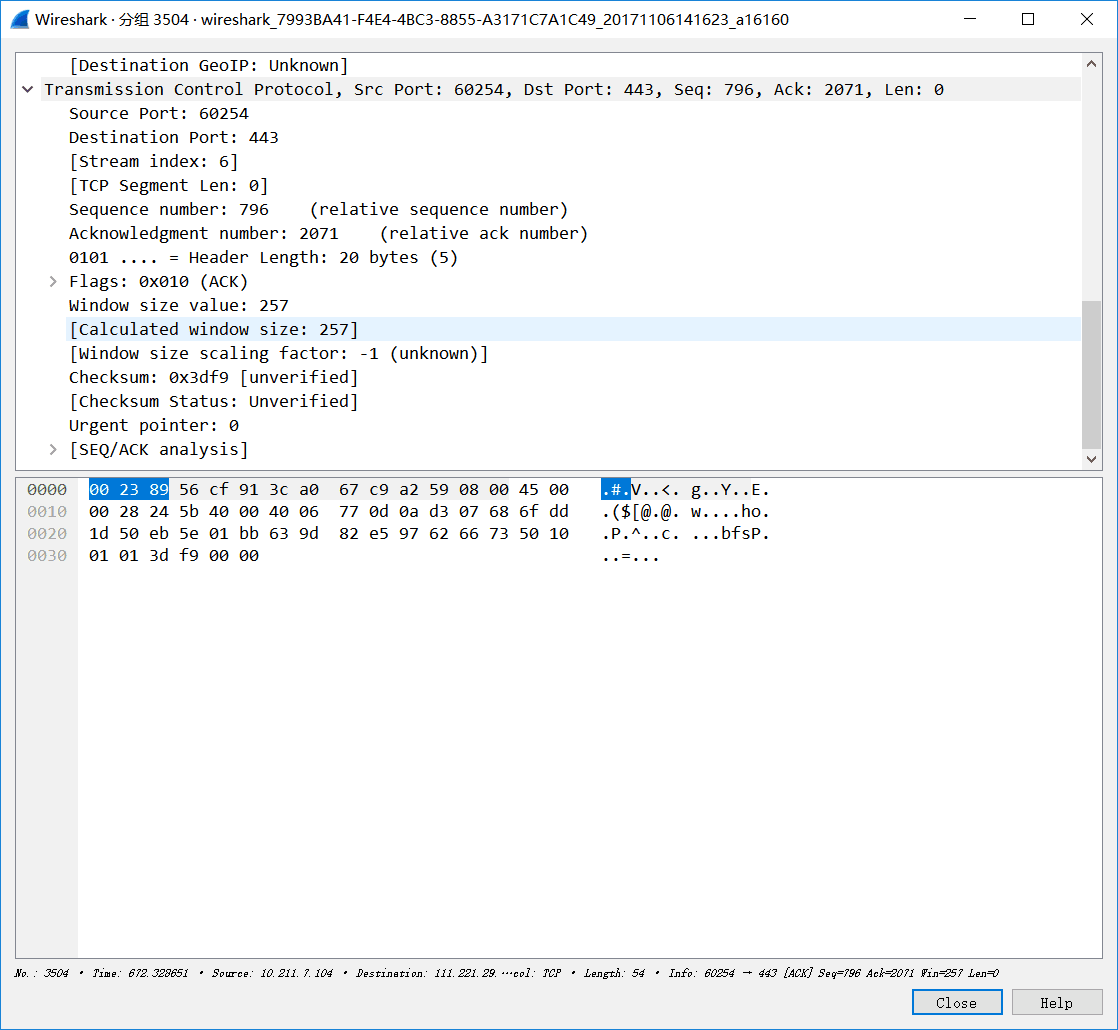
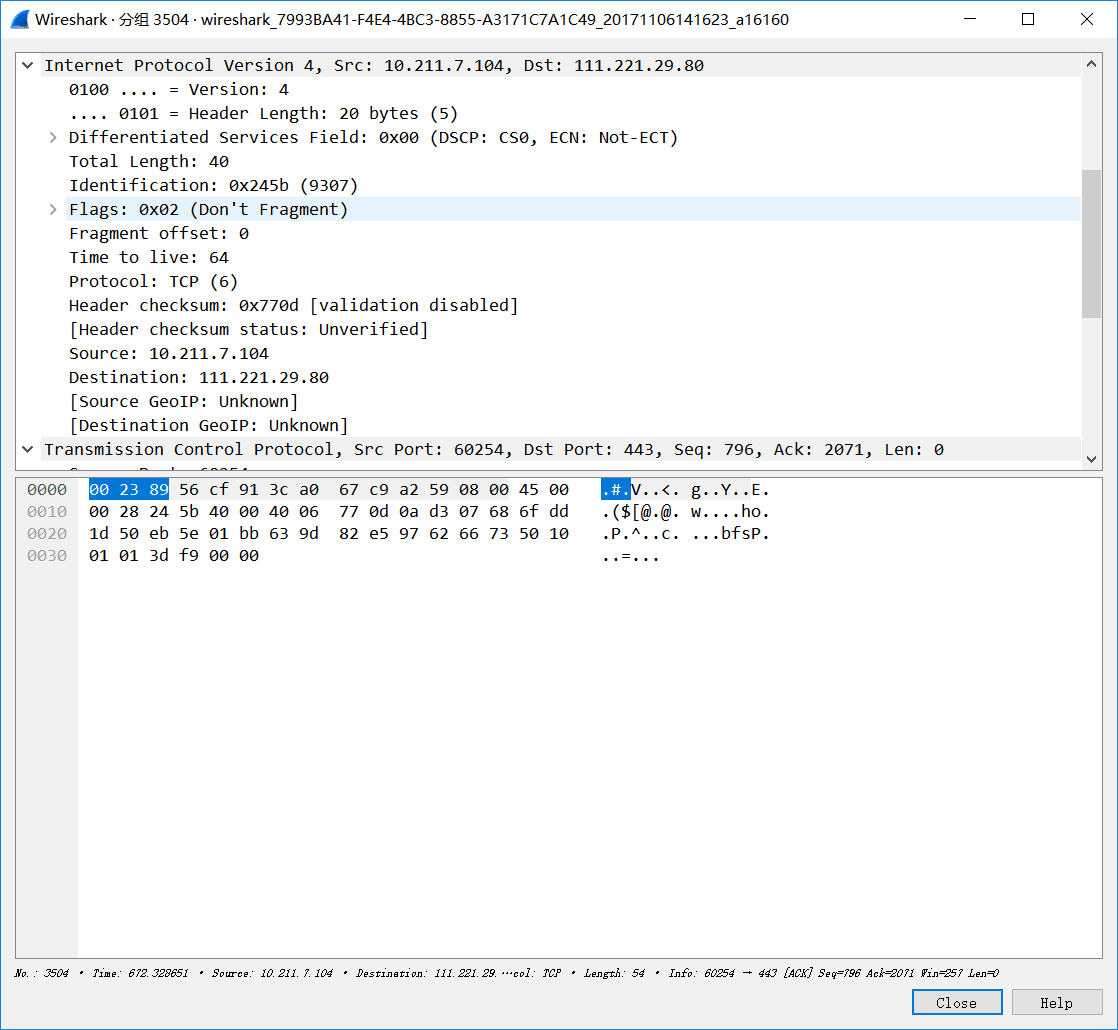
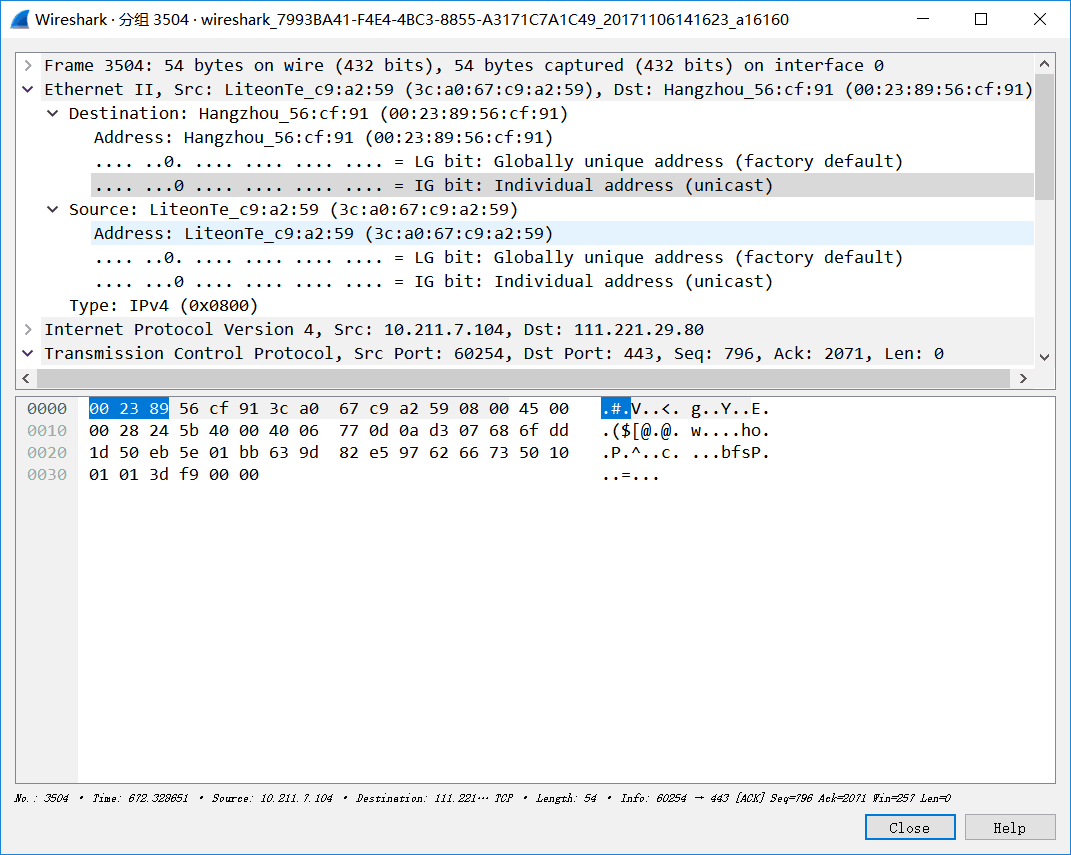


抓取计算机浏览北京邮电大学官网网址<http://www.bupt.edu.cn>时发送接收的数据包：



对于上面的抓包，分别选取其中的一个TCP、UDP进行分析：

1.TCP



Source：10.211.7.104

Destination：111.221.29.80

Length：54

Info：60254—>443[ACK] Seq=796 Ack=2071 Win=257 Len=0

1.1 抓到数据链路层中的帧

Frame 3504 :54bytes

即所抓到的帧序号为3504，大小是54字节

1.2 IP层中的IP数据包

Header Length:20 bytes (5) 即首部长度为20字节

Differentiated Services Field: 0x00 即区分服务

Total length:40 指首部长度和数据之和的长度为40字节；

Identification:0x245b(9307) 标识；

Flag:0x02 标识 此处MF=0，DF=0；

Fragment offset:0 指片偏移为0，表示本片是原分组中的第一片；

Time to live :64说明这个数据报还可以在路由器之间转发64次；

Protocal:TCP(6) 指协议类型为TCP；

Source：源地址：10.211.7.104

Destination:目的地址111.221.29.80

1.3 运输层中的TCP

Source port:60254 即源端口号为60254

Destination port:443 即目的端口为443

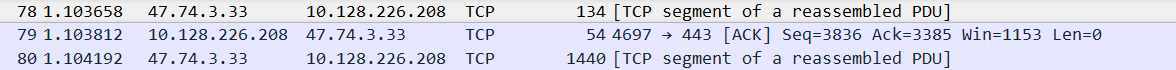
Sequence number:411 序号为411

Acknowledgent number:796 确认号为796

Header length:20 bytes 首部长度为20个字节

Flags:0x010(ACK) 除了确认ACK为1，别的都为0

1.4 关于TCP的三次握手

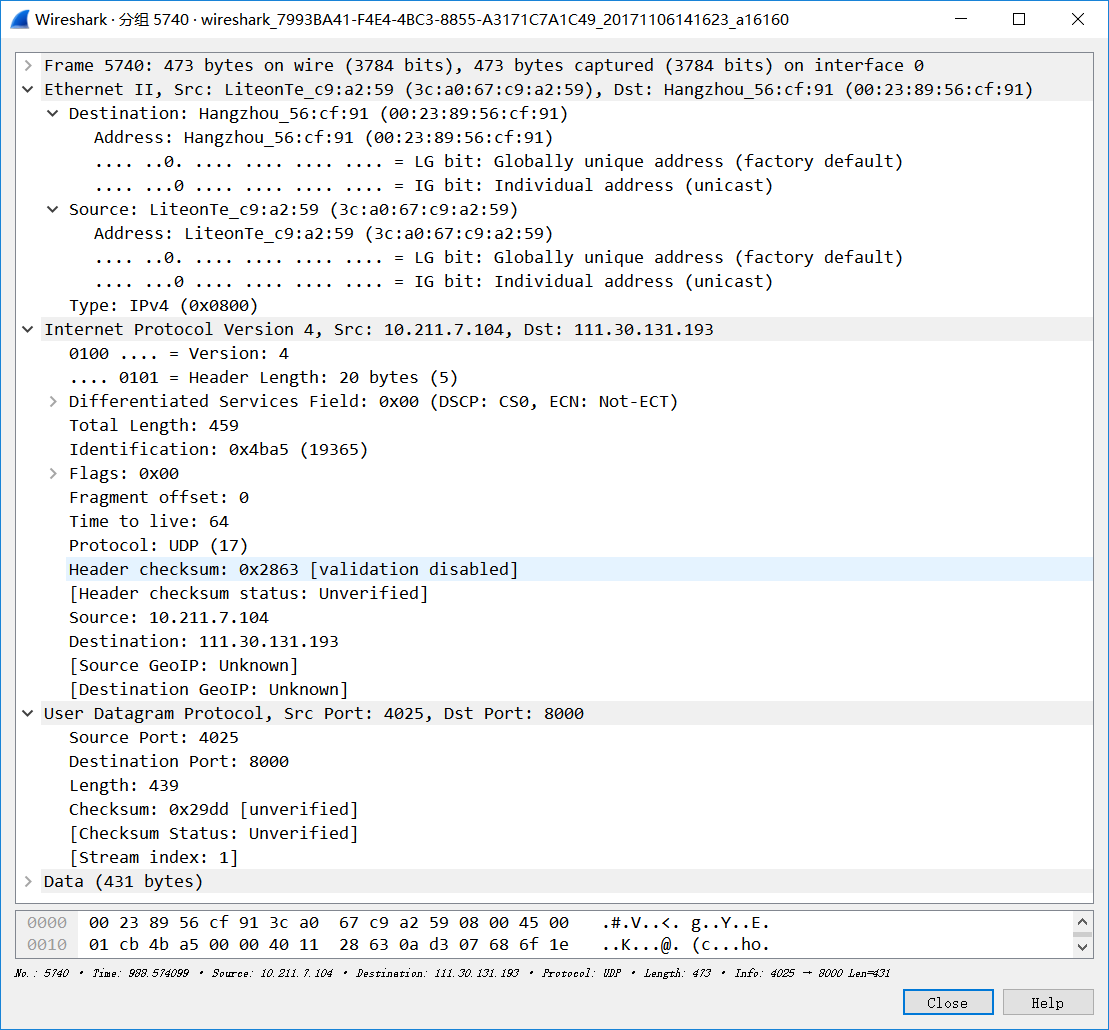




在过滤器中输入IP and tcp可以查看三次握手的情况

由此可以体现出来

2.UDP



Source:10.211.7.104

Destination:111.30.131.193

Protocal:UDP

Length:473

Info:Source port:4025—> Destination port:8000

2.1对抓到的数据链路层中的帧进行分析

Frame 5740:743bytes 即所抓到的帧的序号为5740，大小是743字节

2.2对抓到的IP层中的IP数据报进行分析

Version:4即版本号为4

Header Length:20bytes(5) 即首部长度为20个字节；

Differentiated Services Field:0x00 即区分服务；

Total length:459 指首部长度和数据之和的长度为459字节；

Identification:0x4ba5 (19365) 标识；

Flag:0x00 标识；

Fragment offset:0 指片偏移为0；

Time to live :64 生存时间为64；

Protocal:UDP (17) 指协议类型为UDP；

Header checksum:0x2863[validation disabled] 头部检验和,此处显示禁止校验；

Source：源地址：10.211.7.104

Destination:目的地址111.30.131.193

2.3运输层中的UDP

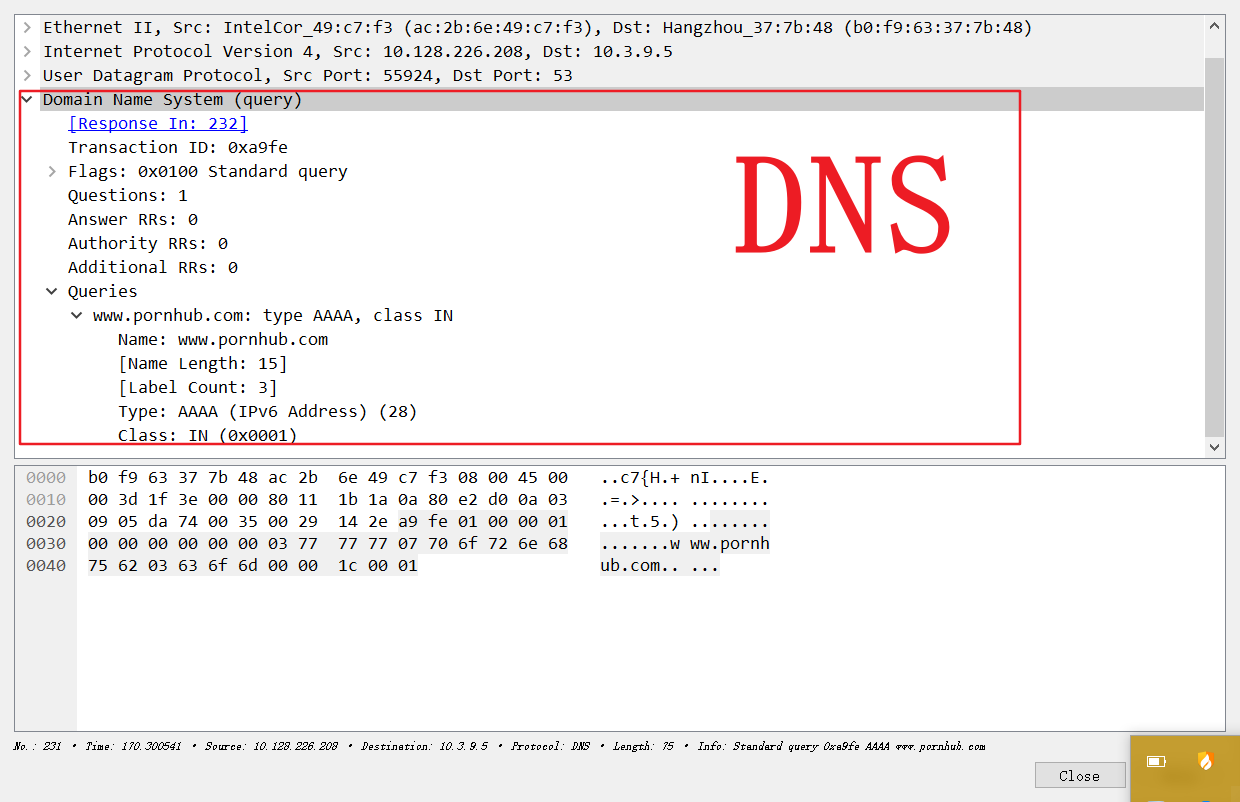
Source port：4025;源端口为4025

Destination port:8000;目的端口8000

Length:439;UDP用户数据报的长度为439

Checksum:0x29dd 校验和 （此处禁止检测）

3. DNS(PornHub 在没有搭建VPN的时候访问异常的状况)



Source:10.128.26.208

Destination:10.3.9.5

Protocal:DNS

Length:75

Info: Standard query 0x496a A [www.pornhub.com](http://www.pornhub.com)

3.1对抓到的数据链路层中的帧进行分析

Frame 160:75 bytes 即所抓到的帧的序号为160，大小是75字节

3.2对抓到的IP层中的IP数据报进行分析

Version:4即版本号为4

Header Length:20bytes(5) 即首部长度为20个字节；

Differentiated Services Field:0x00 即区分服务；

Total length:61 指首部长度和数据之和的长度为61字节；

Identification:0x1f37(7991) 标识；

Flag:0x00 标识；

Fragment offset:0 指片偏移为0；

Time to live :128 生存时间为128；

Protocal:UDP (17) 指协议类型为UDP；

Header checksum:0x1b21[validation disabled] 头部校验和,此处显示禁止校验；

Source：源地址：10.128.226.208

Destination:目的地址10.3.9.5

3.3运输层中的DNS

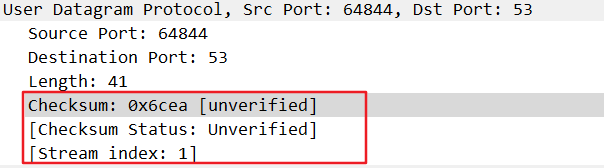
Source port：64844;源端口为64844

Destination port:53;目的端口53

Length:41;DNS用户数据报的长度为41

Checksum:0x6cea 校验和 （此处禁止检测）

附：关于校验和的补充



由于校验和会由网卡计算，wireshark此时抓到的本机发送的数据包校验和会出错，默认关闭。

之后打开校验之后，重新选取一个DNS包，查看checksum项，显示和为0x6cea,且校验正确。

**六、实验心得**

通过这次实验，运用wireshark软件，对不同类型数据包抓取分析后，对各字段组成及含义有了更深的了解，对数据链路层的协议数据单元及功能有了更深的认识。

但其实对于DNS的了解还是不够深入感觉有些无所适从，通过这次实验我又上网查询了关于DNS的概念以及一些工作方式，对DNS有了一些了解。

除此之外还看到了SSLv2 这种从来没听说过的，囿于实验时间也就没有做更深的探索，希望下次实验能够加入这个项目的学习！